February 7, 2019

Grant M. Schneider
Federal Chief Information Security Officer and
Senior Director for Cybersecurity
The White House

Abigail A. Slater
Special Assistant to the President for
Technology, Telecom, and Cyber Policy
The White House

Dear Mr. Schneider and Ms. Slater:

Our organizations, which represent nearly every sector of the U.S. economy, value the relationships that we have established with the National Institute of Standards and Technology (NIST), particularly concerning cybersecurity.

We believe that the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework) has been a remarkable success. It represents one of the best examples of public-private partnerships in action. NIST and multiple stakeholders pride themselves on the Framework's development and promotion at home and overseas.

Our groups want to build on the positive rapport between NIST and industry to strengthen the cybersecurity of the Internet of Things (IoT).[*] We urge the administration and Congress to support NIST in convening a framework-like effort on IoT security. Such a framework will help stakeholders identify a flexible, performance-based, and cost-effective approach that can be voluntarily used by producers, sellers, and users of IoT devices to help them manage cyber risks, data, and privacy.

The Framework was created in response to a 2013 executive order. A comparable trigger is needed, essentially complementing the administration's November 2018 *Botnet Road Map*, to bring about a public-private initiative regarding IoT cybersecurity. Our associations believe that an IoT cyber framework is consistent with NIST's mission. Indeed, stakeholders can build on the quality work that NIST has begun in this space, but policymakers need to elevate it to a higher level. Congress should boost the agency's funding, especially given the array of significant tasks that it undertakes with the private sector on cybersecurity and resilience.

Our organizations are committed to working with industry peers and government officials to identify and tackle challenging IoT cyber issues—including international standardization, botnet mitigation, and risks to supply chains, data, and privacy—in practical and positive ways that encourage others to contribute their time, talent, and resources.

Sincerely,

[*] Draft NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, September 24, 2018.

ACT | The App Association
Advanced Medical Technology Association (AdvaMed)
Alliance of Automobile Manufacturers
American Fuel & Petrochemical Manufacturers (AFPM)
American Trucking Associations (ATA)
Association of Home Appliance Manufacturers (AHAM)
BSA | The Software Alliance
Computer & Communications Industry Association (CCIA)
Consumer Technology Association (CTA)
CTIA—Everything Wireless
Edison Electric Institute (EEI)
Information Technology Industry Council (ITI)
International Society of Automation (ISA)
National Association of Manufacturers (NAM)
National Electrical Manufacturers Association (NEMA)
National Restaurant Association
NCTA—The Internet & Television Association
NTCA—The Rural Broadband Association
Retail Industry Leaders Association (RILA)
Security Industry Association (SIA)
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce
USTelecom—The Broadband Association
Utilities Technology Council (UTC)